SHARDSECURE

Solution Brief

Agentless file-level protection for Google Cloud Platform

Organizations devote significant resources to protecting their data and preventing infrastructure admins, cloud admins, and unauthorized third parties from accessing sensitive data. ShardSecure offers an innovative alternative to agent-based file-level protection with a simple and transparent plug-and-play solution that does not require agents. The ShardSecure platform offers strong data security, privacy, and confidentiality to help organizations protect their data and achieve separation of duties in Google Cloud Platform. ShardSecure allows organizations to streamline processes, mitigate the risk of data exfiltration, and improve security and privacy using a single platform.

Separating data access for confidentiality and compliance

In today's digital environment, companies are under pressure to separate data access from infrastructure owners, cloud administrators, cloud providers, and even unknown services within cloud providers. Data privacy and protection are paramount, and the separation of duties is fundamental to prevent data exfiltration, breaches, and other forms of data compromise.

Historically, organizations have achieved this kind of separation with agent-based file-level encryption solutions. Unfortunately, agent-based solutions are difficult to deploy and maintain in the cloud. These solutions may also have a negative impact on performance and may be incompatible with newer workloads and cloud services.

Separating data access is also an important aspect of compliance for many cross-border data protection laws. The growing number of jurisdictional data privacy regulations is creating hurdles for international organizations looking to adopt cloud technologies like GCP. Specifically, strict cross-border data privacy laws like the EU's General Data Protection Regulation (GDPR), the anticipated Schrems III ruling, and CCPA/CPRA in the US are restricting where user data can be stored and processed. This makes it challenging for organizations to remain compliant and take full advantage of the cloud.

ShardSecure solution overview: file-level protection for Google Cloud Platform

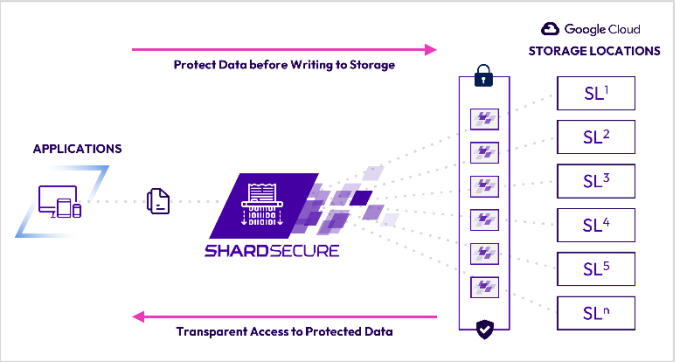
The ShardSecure Platform provides agentless file-level protection in GCP with no performance impacts, no agents, and "set and forget" management. The platform protects unstructured data and metadata in specific files, folders, or storage locations, and it separates this data from infrastructure owners to ensure strong confidentiality. The agentless approach enables organizations to secure their data from internal and external threats without the complexities and overhead of agent-based encryption solutions.

Agentless file-level protection

The ShardSecure platform protects data by splitting it into very small fragments ("microshards") and distributing those fragments to multiple customer-owned GCP storage locations. This approach makes sensitive data unintelligible to unauthorized users, including cloud providers and other infrastructure admins.

ShardSecure does not rely on agents for encryption, which eliminates endpoint management,

deployment/configuration complexities, and degradation in performance. Instead, the ShardSecure platform is deployed as an abstraction layer between existing application and storage infrastructure, where it performs advanced file protection.



Support for data confidentiality and compliance

With ShardSecure, customers can continue to use GCP cloud storage, in the geographic locations and jurisdictions of their choice, to mitigate data transfer risks and address data sovereignty and compliance concerns. Data can be distributed across different regions of GCP or across a hybrid mix of on-premises storage and GCP cloud storage.

ShardSecure also meets the European Data Protection Board's requirements as a supplemental technology to enable cross-border data transfers under the GDPR. The ShardSecure platform is a split processing technology that can be easily deployed in a multi-party processing environment, meaning that it allows organizations to store and process data safely under Use Case 5.

As cyber audit and assurance firm UHY Advisors states: “ShardSecure has the potential to lower cyber risks and compliance costs while maintaining compliance with the spirit of European and US data protection regulations.”

Easy implementation and reduced complexity

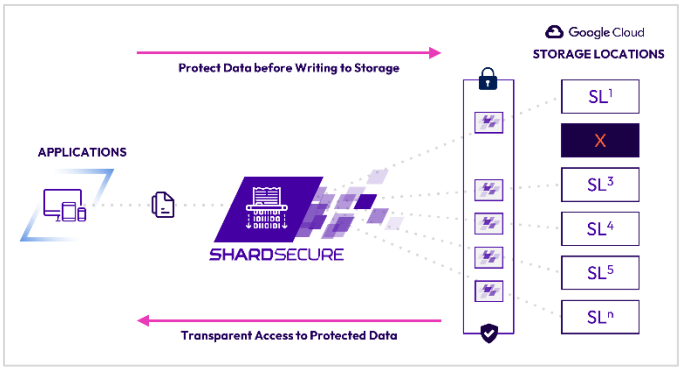
ShardSecure was designed to be easy to manage. With a transparent plug-and-play approach, it supports interfaces like S3 for object storage, iSCSI for block storage, and SMB/NFS for file storage to integrate with any application, server, or other service leveraging cloud storage.

Since the ShardSecure platform acts as an abstraction layer, it can also consolidate multiple cloud storage provider interfaces into one, reducing the complexity associated with migrating to a multi-cloud architecture. Data access also works the same across all clouds without the need to implement specific APIs or connectors.

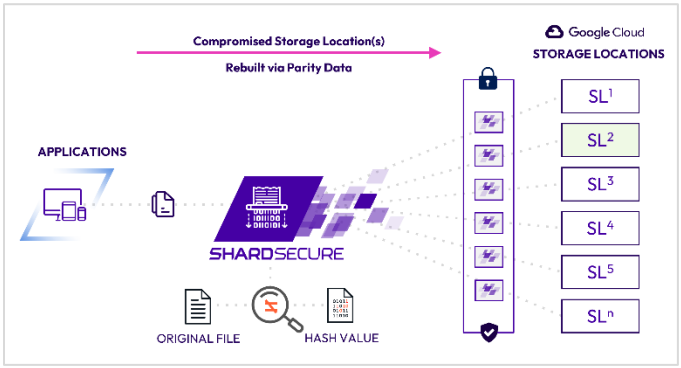
The result is a simple, transparent implementation that does not require agents or changes to user behaviors or data flows.

Self-healing data

Unlike traditional solutions, which often focus on data security and privacy alone, ShardSecure also ensures data integrity. The self-healing feature determines if data is compromised, deleted, tampered with, or encrypted by ransomware.



If a compromise is detected, the platform reconstructs the affected data automatically and transparently, returning it to its last-known good state without costly downtime or disruption to users.



As a result, organizations can maintain their critical operations, avoid security breaches, and prevent any loss of data or data access.

Conclusion

Data security, privacy, and integrity have never been more important, and the threats to organizations have never been greater. Regardless of where sensitive data resides — on-prem, in the cloud, or in a hybrid- or multi-cloud architecture — it needs to be protected and secured. ShardSecure provides this security and privacy while keeping customers in control of their data in Google Cloud Platform.

To learn more about our technology — including its support for robust data resilience, AI/ML model and training data protection, and cloud ransomware mitigation — follow us on social media or visit us online.

@ShardSecure
@ShardSecure
@ShardSecure

101 Avenue of the Americas
9th Floor, New York, NY 10013
United States of America

info@shardsecure.com